对一维复合混沌图像加密算法的安全分析和改进 *

朱淑芹，王文宏

(聊城大学 计算机学院，山东 聊城 252059)

摘　要：最近，Park 等人提出了一种基于一维复合混沌的图像加密算法，该算法的核心思想为：用混沌序列对明文图像进行像素置乱操作；利用混沌序列和密文反馈机制对置乱后的明文序列进行扩散操作；把扩散后的密文序列向左循环移位以得到最终的密文。对该加密算法进行了安全性分析，发现了该算法的两个等效密钥流，从而使得循环移位操作成为无效操作。通过选择明文攻击依次破解出算法中的两个等效密钥流，恢复出了明文图像。理论分析和实验结果验证了选择明文攻击策略的可行性；此外提出了一种改进算法，克服了原有算法的缺陷。改进后的方案不仅能保持原算法的优点，还能抵抗选择明文的攻击。

关键词：混沌；图像加密；密码分析；循环移位；选择明文攻击

中图分类号：TP309.7　　doi: 10.3969/j.issn.1001-3695.2018.01.0101

Cryptanalysis and enhancements of image encryption algorithm based on combination of 1D chaotic map

Zhu Shuqin, Wang Wenhong

(*School of Computer Science*, *Liaocheng University*, *Liaocheng Shandong* 252059, *China*)

Abstract: Recently, Park et al proposed a image encryption algorithm using combination of the 1D chaotic map, the main idea of the encryption algorithm is as follows. First, a chaotic sequence was used to scramble pixel values of plaintext image. Secondly, the chaotic sequence and the ciphertext feedback mechanism are used to diffuse the sequence of the plaintext after the scramble. Finally, the diffused of the ciphertext sequence is shifted to the left to get the final ciphertext. In this paper, we carry out the security analysis of the encryption algorithm, and find the two equivalent key streams of the algorithm, which makes the shift shift operation a invalid operation. By selecting the plaintext attack, we break the two equivalent key streams in the algorithm in turn, so we can restore the plaintext image. Theoretical analysis and experimental results verify the feasibility of the chosen plaintext attack strategy. In addition, we propose an improved algorithm to overcome the defects in the above original algorithm. Experimental results show that the improved scheme can not only maintain the merits of the original one, but also resist the attacks

Key words: chaos; image encryption; cryptanalysis; circular shift; chosen plaintext attack

0　引言

随着互联网技术和多媒体技术的迅速发展，多媒体通信已越来越重要。因此，图像信息的安全问题日益严重。然而，由于图像数据具有数据容量大、冗余度高、相邻像素间相关性强等特点，传统的针对文本设计的加密算法，如 DES、AES 不再适合于图像加密[1]。

混沌是由确定的非线性系统产生的一种复杂的、看似随机的物理现象，其产生的序列是伪随机的，具有非周期性，且表现为高斯白噪声。此外，由于混沌系统对控制参数和初始条件高度敏感，产生的序列不可预测，可以提供巨大的密钥空间。1998 年 Fridrich 提出了具有开创性的替代-扩散加密体系结构[2]，随后被 Chen、Lian and Wong 等人发展为经典的置乱—扩散加密体系结构[3~5]。基于这一经典结构，学者们提出很多改进创新算法，如有改进置换技术的[3~6,8~10]，有改进扩散方法的[7,11,12]，有改进密钥流生成器的[13]。另外，还有在变换域对图像进行加密的[14,15]。但其中一些被证明是不安全的[16~22]。因此，对基于混沌的图像加密方案进行安全性分析是必不可少的。文献[16]通过选择明文攻击的方法破解了 Fridrich[2]的多轮置换–扩散结构算法。文献[17]通过选择明文图像攻击的方法，破解了一种基于三维矩阵置换的图像加密方案；Zhu 等人[18]通过选择明文攻击与选择密文攻击的两种方式破解了一种具有密文反馈机制的

收稿日期：2018-01-30；**修回日期：**2018-03-16　**基金项目：**山东省自然科学基金资助项目(ZR2017MEM019)；聊城大学自然科学基金资助项目(318011606)

作者简介：朱淑芹（1979-），女，讲师，硕士，主要研究方向为混沌理论、图像处理（shuqinzhu2008@163.com）；王文宏（1973-），男，副教授，博士，主要研究方向为图像处理、模式识别、机器视觉.

混沌图像加密算法，致使利用密文反馈机制来抵抗选择明文攻击的方法失效；文献[19]通过选择明文攻击破解了一种基于像素置乱和比特替换的混沌图像加密算法，在破解过程中通过像素值全为零的图像的密文图像与待解密的密文图像作异或运算，恢复出待求明文图像置乱后的序列，使得原算法的比特位替换操作失效，破解方法比较新颖。可以看出这些算法被破解的主要原因是加密系统所用密钥流与待加密图像无关，这就使得加密系统不能抵抗选择明文/密文攻击。

最近，Pak 等人[20]基于一维复合混沌提出了一种图像加密算法，该算法的核心思想是：首先，利用一维复合混沌映射产生的随机序列对明文图像的像素进行位置置乱。其次，对置乱后的图像像素利用密文反馈机制进行扩散操作。最后，把扩散后的密文序列向左循环移动 lp 位以得到最终的密文。（注，这里的整数 lp 可以作为一个密钥。）该算法具有算法复杂度小，抗统计特性分析、对初始条件敏感、抗噪声污染、抗剪切攻击的优点。但通过我们的深入分析发现，该算法还是不能抵抗选择明文的攻击。

1　原加密算法的描述

原算法在加密过程中用到的混沌系统为

$$x_{n+1}=F(\mu,x_n,k)=\mu\times\sin(\pi\times x_n)\times 2^k-floor(\mu\times\sin(\pi\times x_n)\times 2^k) \tag{1}$$

其中: $\mu\in(0,10]$，$k\in[8,20]$为系统的控制参数，x_0 是系统的初始值。加密系统所用到的密钥集 keys= (x_0 , u, k, N_0, lp)。

具体加密步骤如下

a)设待加密的图像为A，大小为$m\times n$，将明文图像A转换为长度为$m*n$的一维序列$P=\{p(1), p(2), p(3), \ldots, p(m*n)\}$。设置系统(1)的初始值$x_0$和参数 μ 、k，迭代$m*n+N_0$次，舍去前N_0个数值以消除暂态效应带来的不良影响，生成一个长度为$m*n$的一维混沌序列$K=\{k(1), k(2), k(3), \ldots, k(m*n)\}$，对混沌序列$K$进行从小到大的排序，产生一个用于记录排序后的序列中各元素在原序列K中所在位置的位置序列$T=\{t(1), t(2), t(3), \ldots, t(m*n)\}$，用它来对明文序列$P$按照式(2)进行位置置乱，得到置乱后的图像序列$P'=\{p'(1), p'(2), p'(3), \ldots, p'(m*n)\}$。

$$p'(i)=p(t(i)) \tag{2}$$

b)对混沌序列K作如式(3)的操作，得到序列$D=\{d(1), d(2), d(3), \ldots, d(m*n)\}$

$$d(i)=\mathrm{mod}(floor(k(i)\times 10^{14}),256) \tag{3}$$

c)利用序列D对置乱后的图像序列P'进行式(4)-(5)的扩散操作得到中间密文序列$C=\{c(1), c(2), c(3), \ldots, c(m*n)\}$

$$c(1)=\mathrm{mod}(p'(1)+d(1),256) \tag{4}$$

$$c(i)=\mathrm{mod}(p'(i)+d(i),256)\oplus c(i-1) \tag{5}$$

d)对中间密文序列C按照式(6)进行向左循环移位得到最终的密文序列$C'=\{c'(1), c'(2), c'(3), \ldots, c'(m*n)\}$，将其转化为$m\times n$矩阵，即得密文图像。这里$lp\in[1,m*n]$，是密钥集的一部分。

$$\begin{cases} c'(i-lp)=c(i), if\ i-lp\ge 1 \\ c'(i-lp+m*n)=c(i), if\ i-lp<1 \end{cases} \tag{6}$$

2　原算法的密码分析

密码分析是分析、破解密码的一门科学，是在不知道密钥的情况下，设法恢复出密钥，或者恢复出相关明文。根据Kerchhoff原则，密码系统的安全性仅仅依赖于密钥的安全，假设密码分析者知道除密钥以外的所有可能信息。根据密码分析者知道信息的多少，由难到易，密码攻击有以下四种类型[21]：唯密文攻击；已知明文攻击；选择明文攻击；选择密文攻击。

所谓选择明文攻击就是攻击者暂时获得加密机的使用权，他能加密任意的明文，并获得相对应的密文，以此破译出全部或部分明文和密钥[5]。

从原算法的加密过程可以看出整个加密算法的等效密钥就是两个序列T和D以及常数lp。且原算法中的式(6)可以用同余公式表示为

$$\begin{cases} c'(i)=c((i+lp)\mathrm{mod}(m*n)) \\ c'(m*n-lp)=c(m*n) \end{cases} \tag{7}$$

在进行选择明文攻击之前，先定义原加密算法的另外的两个等效密钥序列$T'=\{t'(1), t'(2), t'(3), \ldots, t'(m*n)\}$和$D'=\{d'(1), d'(2), d'(3), \ldots, d'(m*n)\}$。显然，这里定义的序列$T'$和$D'$是原算法中的密钥序列$T$和$D$分别向左循环移$lp$位得到的结果。

$$\begin{cases} t'(i)=t((i+lp)\mathrm{mod}(m*n)) \\ t'(m*n-lp)=t(m*n) \end{cases} \tag{8}$$

$$\begin{cases} d'(i)=d((i+lp)\mathrm{mod}(m*n)) \\ d'(m*n-lp)=d(m*n) \end{cases} \tag{9}$$

另外，再定义序列$P''=\{p''(1), p''(2), p''(3), \ldots, p''(m*n)\}$。同样，这里定义的序列$P''$是原算法中置乱后的图像序列$P'$左循环移$lp$位的结果。

$$\begin{cases} p''(i)=p'((i+lp)\mathrm{mod}(m*n)) \\ p''(m*n-lp)=p'(m*n) \end{cases} \tag{10}$$

用置乱序列$T'=\{t'(1), t'(2), t'(3), \ldots, t'(m*n)\}$直接对原明文图像序列$P=\{p(1), p(2), p(3), \ldots, p(m*n)\}$进行置乱，置乱后的结果记为$P_t$，即

$$p_t(i)=p(t'(i)) \tag{11}$$

则　　　　Pt=P′′　　(12)

也就是说先对置乱序列进行向左循环移位，再对图像序列置乱；先对图像序列置乱，再对置乱后得序列进行向左循环移

位。两种操作效果是一样的。例如,设移位的位数lp=5，序列的长度$m*n$=9。示例如表1。这里T表示原置乱序列，T'表示T循环左移5位的结果，P表示原明文序列，P'表示用T把P置乱的结果，P''表示P'循环左移5位的结果，P_t表示用T'把P置乱的结果。从表1可以看出$P_t=P''$。

表1 P_t与P''相等的算例

T=	9	3	4	6	7	1	8	2	5
p=	23	25	128	231	214	112	118	136	190
P'=	190	128	231	112	118	23	136	25	214
P''=	23	136	25	214	190	128	231	112	118
T'=	1	8	2	5	9	3	4	6	7
P_t=	23	136	25	214	190	128	231	112	118

根据上面的分析结果，结合原算法的式(4)~(6)和式(7)~(12)，原加密算法公式可以改写为

$$\begin{aligned} c'(1) &= c((1+lp)\bmod(m*n)) \\ &= \bmod(p'((1+lp)\bmod(m*n))+ \\ &\quad d((1+lp)\bmod(m*n)),256)\oplus c(lp) \\ &= \bmod(p''(1)+d'(1),256)\oplus c'(m*n) \\ &= \bmod(p_t(1)+d'(1),256)\oplus c'(m*n) \end{aligned} \tag{13}$$

$$\begin{aligned} c'(i) &= c((i+lp)\bmod(m*n)) \\ &= \bmod(p'((i+lp)\bmod(m*n))+ \\ &\quad d((i+lp)\bmod(m*n)),256)\oplus c((i-1+lp)\bmod(m*n)) \\ &= \bmod(p''(i)+d'(i),256)\oplus c'(i-1) \\ &= \bmod(p_t(i)+d'(i),256)\oplus c'(i-1) \end{aligned} \tag{14}$$

由式(13)(14)可以看出，原加密算法的等效密钥由两个序列T和D以及常数lp转化为两个序列T'和D'。只要把序列T'和D'破解出来，原加密算法也就破解了。而加密任何明文图像所用序列T'和D'是固定的，因此可以采用选择明文攻击的方法把序列T'和D'破解出来。选择明文攻击的流程图如图1所示。

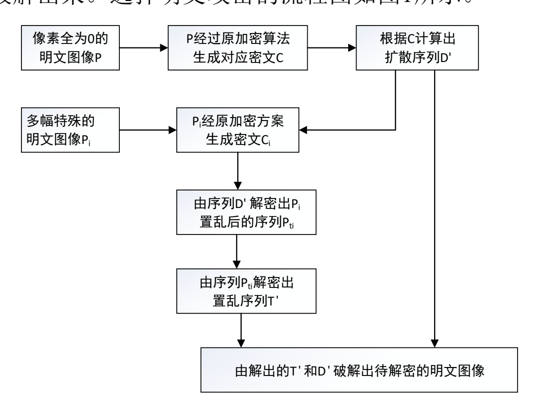


图1原算法选择明文攻击流程图

2.1 序列 D′ 的破解

选择一幅与待破解的密文图像同样大小的像素值全为零的图像，设其大小为$m×n$，用原算法加密后得到其对应的密文图像C′，由于置乱操作对像素值全为零的图像不起作用，经置乱后得到的P_t={0,0，…,0},这时的式(13)(14)就变为

$$c'(1)=\bmod(d'(1),256)\oplus c'(m*n)=d'(1)\oplus c'(m*n) \tag{15}$$

$$c'(i)=\bmod(d'(i),256)\oplus c'(i-1)=d'(i)\oplus c'(i-1) \tag{16}$$

由式(15)(16)解出D'

$$d'(1)=\bmod(d'(1),256)\oplus c'(m*n)=c'(1)\oplus c'(m*n) \tag{17}$$

$$d'(i)=c'(i)\oplus c'(i-1) \tag{18}$$

举例来说，假设明文序列的长度为 12，用原算法加密特殊明文 P={ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0}，得到密文 C'=[123, 156, 23, 78, 56, 98, 234, 16, 29, 112, 62, 221]，则有 D'=[166, 231, 139, 89, 118, 90,136, 250, 13, 109, 78, 227]。

2.2 序列 T′的破解

破解出了序列D'，可以利用公式(19)-(20)就可以求出P_t，

$$p_t(1)=\bmod((c'(1)\oplus c'(m*n)-d'(1)),256) \tag{19}$$

$$p_t(i)=\bmod((c'(i)\oplus c'(i-1)-d'(i)),256)\quad i=2,3,\ldots m*n \tag{20}$$

然后根据T′就可以恢复出明文序列了。

如果向量 T' 的长度 $z=m*n$ 小于 256，则只需选择一幅明文序列 P={1, 2, …, $m*n$ }，就可以恢复出序列 T'。

假设 T'的长度 z=12，用原算法加密明文序列 P={1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12}，得到对应的密文序列 C'={107, 234, 13, 34, 125, 86, 97, 128, 59, 110, 131, 12}。

根据式(19)和(20)以及3.1小节求出来的D'，可以求出序列P_t={ 9, 5, 11, 7, 3, 6, 10, 2, 8,12, 1, 4}。因此置乱序列T'={ 9, 5, 11, 7, 3, 6, 10, 2, 8,12, 1, 4}。

如果向量 T'的长度 mn 大于 256，则要依次选择大小为 $m×n$ 的 KL=「mn/255」幅明文图像(这里「x」表示取大于或等于 x 的最小整数)，每次选择的明文图像序列的像素取值形式如图 2 所示。

第一幅选择的明文

i=1	2	…	255	256	257	…	…	z-1	z
1	2	…	255	0	0	…	…	0	0

第二幅选择的明文

i=1	2	…	255	256	…	510	511	z-1	z
0	0	…	0	1	…	255	0	0	0

第 KL 幅选择的明文(最后一幅选择的明文)

i=1	2	…	…	z-k-1	z-k	z-k+1	z-k+2	z-1	z
0	0	…	…	0	0	1	2	…	k

图 2 破解置乱的等效密钥流 T' 所选择的多幅明文图像序列

由图 2 可以看出每一幅选择明文图像中仅有一个子块的像素取值为[1,255]范围内互不相同的整数，其余子块的像素均为 0，这样就得到 KL=「mn/255」幅明文图像。具体步骤如下：

a)依次加密上图中选取的明文图像，得到的密文图像分别

为$C'_1, C'_2, \ldots, C'_{KL}$。利用3.1节方法依次恢复出图1明文图像对应的置乱序列后的序列$P_{t1}, P_{t2}, \ldots, P_{tKL}$。

b)根据明文图像置乱后的序列$P_{t1}, P_{t2}, \ldots, P_{tKL}$作如下操作：先建立一个元素全为0，长度为$m*n$的一维序列T′，对于第一个置乱序列$P_{t1}$，如果$P_{t1}(i)=j$那么$T'(i)=j$；对于第$h$个序列$P_{th}$，如果$P_{th}(i)=j$ 且$T'(i)$仍然还等于0，那么$T'(i)=255*(h-1)+j$。其中i=1, 2, 3, …, $m*n$；j=1, 2, 3, …, 255；　h=1, 2, 3, …, KL。则所得序列T'就是置乱序列。

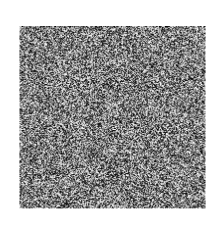
为了便于编程，可以用序列$P_{t1}, P_{t2}, \ldots, P_{tKL}$构成一个$KL$行，$mn$列的大矩阵R，其中$P_{t1}$为矩阵R的第一行，$P_{t2}$为矩阵R的第二行，…，$P_{tKL}$为矩阵R的最后一行。这样破译出置乱过程的等效密钥流T′的*matlab*伪代码描述为

```
T′=zeros(1，mn);
for h=1:KL
     for i=1:mn
         if    R(h, i)~=0&& T′(i)==0
               T′(i)=255*(h-1)+ R(h, i)
         end
     end
end
```

这样就得到置乱阶段的等效密钥流 T'。利用 T' 把 2.1 节恢复出来的序列 P_t 还原为序列 P，即得明文图像。

2.3　密文破译仿真实验

仿真实验采用MATLAB 2014a平台，取密钥集keys= (x_0，u，k，N_0，lp)=(0.87432, 2.4398, 14, 2398, 2431)，采用原算法加密大小为256×256的256级灰度图像cameraman，得到对应的密文图像3(a)所示。各参数不变，用原算法分别加密大小为256×256的像素值全为0的全黑图像，得到对应的密文图像如图4(b)，把图4(b)转化为一维序列，利用式(17)(18)可以解密出D'。最后通过多幅选择明文图像攻击的方法恢复出置乱序列T'，从而在不知道密钥的情况下恢复出明文图像，如图3(*b*)所示。


(a)


(b)

图 3(a) 密文图像；(b)解密后的明文图像


(a)

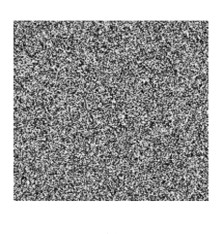

(b)

图4(a)像素值为0的全黑图像；(b)全黑图像的密文图像

3　改进算法及其安全性分析

3.1　改进算法

原算法被破解的主要原因在于原加密算法的等效密钥序列T和D以及常数lp与明文图像无关。因此提出以下的改进算法，改进算法的密钥集与原算法的密钥集完全一样，但改进算法能抵抗选择明(密)文的攻击。具体步骤如下：

a)与原算法的步骤a)完全一样，用混沌系统(1)生成一个长度为$m*n$的一维混沌序列$K=\{k(1), k(2), k(3), \ldots, k(m*n)\}$，对混沌序列$K$进行从小到大的排序，产生一个用于记录排序后的序列中各元素在原序列K中所在位置的位置序列$T=\{t(1), t(2), t(3), \ldots, t(m*n)\}$，用它来对明文序列$P$按照式(2)进行位置置乱，得到置乱后的图像序列$P'=\{p'(1), p'(2), p'(3), \ldots, p'(m*n)\}$。

b)对置乱后的图像序列P'做扩散操作，为使得密钥序列与明文相关，与原算法相比，改进算法增加了式(23)~(24)。由式(21)~(25)得到中间密文序列$C=\{c(1), c(2), c(3), \ldots, c(m*n)\}$。

$$d(1)=\mathrm{mod}(lp,256) \tag{21}$$

$$c(1)=\mathrm{mod}(p'(1)+d(1),256) \tag{22}$$

$$d(i)=\mathrm{mod}\left[floor(k(i)\times c(i-1))\times 10^{14}),256\right] \quad ,\quad i=2,3,\ldots,m*n \tag{23}$$

$$kt(i)=floor(d(i)/256*(i-1))+1 ,\quad i=2,3,\ldots,m*n \tag{24}$$

显然，这里$kt(i)$□[1, i-1]

$$c(i)=\mathrm{mod}(p'(i)+d(i),256)\oplus c(kt(i)) \tag{25}$$

c)与原算法的最后一步完全一样，利用式(6)对中间密文序列C进行向左循环移lp位，得到最终的密文序列$C'=\{c'(1), c'(2), c'(3), \ldots, c'(m*n)\}$，将其转化为$m\times n$矩阵即得密文图像。

3.2　改进算法的安全性分析

原算法的安全性分析表明，原算法具有密文分布均匀、相邻像素相关性很小、密文对密钥，对明文敏感的优点。改进算法与原算法的区别在于：中间的等效密钥流D的生成与中间密文相关，而且计算$c(i)$时随机的采用$c(kt(i))$进行反馈，其余步骤与原算法完全一样，故改进算法也具有原算法的上述优点，在此就不赘述。本文只分析改进算法抵抗选择明文攻击的能力。

抵抗选择明文攻击的能力分析。从式(24)可以看出 $kt(i)$的生成与$d(i)$相关，而从式(23)可以看出序列D=$\{d(1), d(2), d(3), \ldots, d(m*n)\}$的生成与中间密文 C 相关，加密不同的明文图像所用的序列 D 是不同的，所以 $kt(i)$的生成与明文图像相关。也就是说，加密不同的图像所用序列 D 和 $kt(i)$是不同的，算法可以达到“一次一密”的效果，可以抵抗选择明文的攻击。

4　结束语

本文对基于一维混合混沌映射的图像加密算法进行了安全性分析，发现该算法不能抵抗选择明文的攻击，在攻击过程中

通过选择一幅特殊的明文图像破解出原算法的等效密钥序列D′，再通过多幅选择明文攻击破解出等效置乱序列T'，使得算法的循环移位操作失效。具体的简单算例和仿真实验演示了所提出的攻击方法的有效性。针对原算法不能抵抗选择明文攻击的缺陷，对加密算法做了改进，使改进算法能抵抗选择明文的攻击。改进算法的创新性在于加密系统的密钥集是固定的，但加密不同的图像所用的等效序列D′不同，具有“一次一密”的效果，但是没有“一次一密”密码系统中密钥管理的难度。

参考文献：

[1] Alvarez G, Li Shujun. Some basic cryptographic requirements for chaos-based cryptosystem [J]. International Journey of Bifurcation and Chaos, 2006, 16 (8): 2129–2151.

[2] Fridrich J. Symmetric ciphers based on two-dimensional chaotic maps [J]. International Journey of Bifurcation and Chaos, 1998, 8 (6): 1259–1284.

[3] Chen Guanrong, Mao Yaobin, Chui C A. symmetric image encryption scheme based on 3D chaotic cat maps [J]. Chaos Solitons and Fractals, 2004, 21 (3): 749–761.

[4] Lian Shiguo, Sun Jinsheng, Wang Zhiquan. A block cipher based on a suitable use of the chaotic standard map [J]. Chaos Solitons and Fractals, 2005, 26 (1): 117–129.

[5] Wong K W, Kwok S H, Law W S. A fast image encryption scheme based on chaotic standard map [J]. Physics Letters A, 2008, 372 (15): 2645–2652.

[6] Belazi A, El-Latif A A A, Belghith S. A novel image encryption scheme based on substitution–permutation network and chaos [J]. Signal Processing, 2016, 128: 155–170.

[7] 韩凤英，朱从旭. 新型置换和替代结构的图像混沌加密算法 [J]. 武汉大学学报：理学版，2014, 60 (5): 447-452. (Han Fengying, Zhu Congxu. New permutation-substitution image encryption scheme based on chaos [J]. Journal of Wuhan University, 2014, 60 (5): 447-452.)

[8] Fu Chong, Lin Binbin, Miao Yusheng etal. A novel chaos-based bit-level permutation scheme for digital image encryption [J]. Optics Communications, 2011, 284 (23): 5415–5423

[9] Zhu Zhiliang, Zhang Wei, Wong K W etal. A chaos-based symmetric image encryp-tion scheme using a bit-level permutation [J]. Information Sciences, 2011, 181 (6): 1171–1186.

[10] Chen Junxin, Zhu Zhiliang, Fu Chong etal. An efficient image encryption scheme using gray code based permutation approach [J]. Optics and. Lasers in Engineering, 2015, 67: 191–204

[11] 文昌辞，王沁，黄付敏，等. 基于仿射和复合混沌的图像自适应加密算法 [J]. 通信学报，2012, 33 (11): 119-127. (Wen Changci, Wang Qin, Huang Fumin etal. Self-adaptive encryption algorithm for image based on affine and composed chaos [J]. Journal on Communications, 2012, 33 (11): 119-127)

[12] Zhang Yushu, Xiao Di. An image encryption scheme based on rotation matrix bit-level permutation and block diffusion [J]. Communications in Nonlinear Science and Numerical Simulation, 2014, 19 (1): 74-82

[13] Mirzaei O, Yaghoobi M, Irani H. A new image encryption method: parallel sub-image encryption with hyper chaos [J]. Nonlinear Dynamics, 2012, 67 (1): 557–566.

[14] Chen Junxin, Zhu Zhiliang, Fu Chong, *et al.* Optical image encryption scheme using 3D chaotic map based joint image scrambling and random encoding in gyrator domains [J]. Optics Communications, 2015, 341: 263–270.

[15] Annaby M H, Rushdi M A, Nehary E A. Image encryption via discrete fractional Fourier-type transforms generated by random matrices [J]. Signal Processing Image Communication, 2016, 49: 25-46.

[16] Solak E, Cokal C, Yildiz O, *et al.* Cryptanalysis of Fridrich's chaotic image encryption [J]. International Journal of Bifurcation and Chaos, 2010, 20 (5): 1405-1413.

[17] Wu Jiahui, Liao Xiaofeng, Yang Bo. Cryptanalysis and enhancements of image encryption based on three-dimensional bit matrix permutation [J]. Signal Processing, 2018, 292-300

[18] Zhu Congxu, Liao Chunlong, Deng Xiaoheng. Breaking and improving an image encryption scheme based on total shuffling scheme [J]. Nonlinear Dynamics, 2013, 71 (1-2): 25-34

[19] 朱淑芹，王文宏，李俊青. 对像素置乱和比特替换的混沌图像加密算法的破解 [J]. 计算机应用，2017, 37 (12): 44-47. (Zhu Shuqin, Wang Wenhong, Li Junqing. Breaking a chaotic image encryption algorithm based on pixel scrambling and bit substitution [J]. Journal of Computer Applications, 2017, 37 (12): 44-47.

[20] Pak C, Huang Lilian. A new color image encryption using combination of the 1D chaotic map [J]. Signal Processing, 2017, 138: 129-137

[21] Wang Xingyuan, Lin Teng, Xue Qin. A novel colour image encryption algorithm based on chaos [J]. Signal Processing, 2012, 92 (4): 1101-1108.